【 43 】

氏名	土 井　　洋
授与した学位	博　　士
専攻分野の名称	理　　学
学位授与番号	博甲第２１２４号
学位授与の日付	平成１２年　９月３０日
学位授与の要件	自然科学研究科システム科学専攻 （学位規則第４条第１項該当）
学位論文の題目	Structured Multisignature Schemes （署名構造に適応可能な多重署名方式）
論文審査委員	教授　田坂　隆士　　教授　三村　　護　　教授　田村　英男

学位論文内容の要旨

下記の二つの研究をまとめる.

1章　様々な署名構造に適用可能な多重署名方式の提案とその安全性

複数の署名者が同一文書に署名を行う場合，それぞれの署名者の立場や責任は一般に同一ではなく，立場や責任の違いが署名生成の処理順序（署名構造）の違いに反映されることが多い．本章では，様々な署名構造に適用可能な多重署名方式を２つ提案する．１つはElGamal型署名を応用した方式であり，もう１つはRSA署名を応用した方式である.

提案方式の安全性については，鍵配布センタと信頼のおける署名者を除いた全署名者が結託するという仮定の下に，攻撃を関数として記述し，多重署名への攻撃関数と，ベースとなる署名方式への攻撃関数との帰着関係を調べた.

特に署名の偽造と署名構造の偽造については，情報理論的考察を経て，多重署名への攻撃関数とベースとなる署名方式への攻撃関数との（平均的多項式時間 Turing ）帰着関係を示した.

2章　最も対称的な非特異平面６次曲線の一意性

非特異平面曲線に対して，その射影自己同型群の位数で対称性を評価することとする．すると，最も対称的な(射影自己同型群の位数が最大となる)非特異６次曲線は， Wiman 曲線 $f_6 = 27z^6 - 135z^4xy - 45z^2x^2y^2 + 9z(x^5 + y^5) + 10x^3y^3$ と射影同値であることを示す.

証明では，正則自己同型群の群構造を解析し，部分群の位数に関する条件を使って，６次曲線の形式を絞っていくという手法を用いた．しかし，複雑な多項式の計算が必要となる．そこで，C++言語で多項式クラスライブラリを設計し，これらの計算を行うことにより，最終的に主張の証明を得た.

論文審査結果の要旨

本論文では，下記の二つの研究をまとめている．

1章　様々な署名構造に適用可能な多重署名方式の提案とその安全性

複数の署名者が同一文書に署名を行う場合，それぞれの署名者の立場や責任は一般に同一ではなく，立場や責任の違いが署名生成の処理順序（署名構造）の違いに反映されることが多い．本章では，様々な署名構造に適用可能な多重署名方式を2つ提案している．1つはElGamal型署名を応用した方式であり，もう1つは RSA署名を応用した方式である．

提案方式の安全性については，鍵配布センタと信頼のおける署名者を除いた全署名者が結託するという仮定の下に，攻撃を関数として記述し，多重署名への攻撃関数と，ベースとなる署名方式への攻撃関数との帰着関係を調べている．督に署名の偽造と署名構造の偽造ついては，情報理論的考察を経て，多重署名への攻撃関数とベースとなる署名方式への攻撃関数との（平均的多項式時間 Turing）帰着関係を示している．

2章　もっとも対称的な非特異平面6次曲線の一意性

非特異平面曲線に対して，その射影自己同型群の位数で対称性を評価することとする．すると，もっとも対称的な（射影自己同型群の位数が最大となる）非特異6次曲線は，射影同値を除いて一意的であることを示している．

このように，本論文の多重署名方式の提案とその安全性の証明は，この分野の研究に寄与すること大である．よって本論文は博士（理学）の学位に値するものと認める．